



# Seitsemän toimenpidettä



joilla yritykset voivat valmistautua  
yleiseen tietosuoja-asetukseen

## Kohderyhmä

Oppaan tavoitteena on auttaa sellaisia yrityksiä, joiden ydinliiketoimintaan ei kuulu henkilötietojen käsittely. Kyse on esimerkiksi pk-yrityksistä, jotka käsittelevät pääasiassa työntekijöidensä henkilötietoja tai asiakasluetteloita. Näitä ovat esimerkiksi kauppiaat tai liikkeet, kuten lihakauppiaat tai leipomot, tai palveluntarjoajat, kuten arkkitehdit. Oppaassa esitellään tarpeelliset toimenpiteet, joilla yritykset voivat valmistautua yleiseen tietosuoja-asetukseen.

Henkilötietoja ovat kaikki luonnollisia henkilöitä (ei siis oikeushenkilöitä) koskevat tiedot, kuten esimerkiksi nimi, sukunimi, kotiosoite, sähköpostiosoite tai matkapuhelimen kartan sijaintitiedot. Yleensä kyse on tiedoista, joita yrityksellä voi olla työntekijöistään, asiakkaistaan tai toimittajistaan.

Mitä  
pienempi  
riski yrityksen  
toiminnoista  
kohdistuu  
henkilötietoihin,  
sitä vähemmän  
velvollisuuksia sillä on

### Tärkeimmät periaatteet:

- 👤 **kerää henkilötietoja selkeästi määriteltyyn tarkoitukseen äläkä käytä niitä muihin tarkoituksiin** (jos pyydät asiakkaan sähköpostiosoitteen tarjousten lähettämiseksi, et voi käyttää osoitetta muuhun tarkoitukseen etkä myydä sitä toiselle yritykselle);
- 👤 **kerää vain tarvitsemiasi tietoja** (esimerkiksi kotiinkuljetusta varten tarvitet osoitteen ja ovisummerissa lukevan nimen, mutta et tarvitse tietoa asiakkaan siviilisäädystä). Mieti siis tarkkaan, mitä tietoja käsittelet.

## TOIMENPIDE 1

### TARKISTA KERÄÄMÄSI HENKILÖTIEDOT JA KERUUPROSESSI, KÄSITTELYN TARKOITUS JA OIKEUSPERUSTA

Sinulla on **työntekijöitä**. Käsittelet työsopimuksessa olevia henkilötietoja lakisääteisten velvoitteiden pohjalta (esim. ilmoitukset veroviranomaisille/sosiaaliturvajärjestelmään).

Sinulla saattaa olla luettelo **yksittäisistä asiakkaista**, jotta voit esimerkiksi lähettää heille erikoistarjouksia ja mainoksia, jos sinulla on tähän asiakkaiden suostumus.

Aina suostumus ei ole tarpeen. Joissain tapauksissa henkilöt odottavat sinun käsittelevän heidän tietojaan. Esimerkiksi

pitsakauppias voi käyttää toimitusosoitteita uusien tuotteiden mainostamiseen. Tätä kutsutaan oikeutetuksi eduksi. Sinun on ilmoitettava henkilölle siitä, mihin aiot tietoja käyttää, ja lopetettava kyseisten tietojen käsittely näiden pyynnöstä.

Jos sinulla on luettelo **toimittajista** tai **yrittäjäasiakkaista**, tietojen käsittely tapahtuu heidän kanssaan tekemäsi sopimuksen pohjalta. Sopimusten ei tarvitse välttämättä olla kirjallisia.

## TOIMENPIDE 2

### ILMOITA ASIAKKAILLE, TYÖNTEKIJÖILLE JA MUILLE HENKILÖILLE, ETTÄ KERÄÄT HEIDÄN HENKILÖTIETOJAAN

Henkilöiden on tiedettävä, että käsittelet heidän henkilötietojaan ja mihin tarkoitukseen niitä käsitellään.

Ilmoitus ei ole tarpeen, jos henkilöt tietävät jo tietojen käyttötarkoituksen, kuten silloin, kun asiakas on tilannut kotiinkuljetuksen.

Sinun on pyynnöstä ilmoitettava henkilöille, mitä heitä koskevia henkilötietoja sinulla on, sekä annettava heille pääsy omiin tietoihinsa. Pidä tiedot järjestyksessä, jotta pystyt ilman suurempaa vaivaa vastaamaan esimerkiksi työntekijän kysymyksiin siitä, millaisia tietoja sinulla on hänestä.

## TOIMENPIDE 3

### SÄILYTÄ HENKILÖTIETOJA VAIN NIIN KAUAAN KUIN SE ON VÄLTÄMÄTÖNTÄ

**Työntekijätiedot:** työsuhteen keston ja lakisääteisten velvoitteiden edellyttämän ajan.

**Asiakastiedot:** asiakassuhteen keston ja lakisääteisten velvoitteiden edellyttämän ajan (esimerkiksi verotustarkoituksiin).

Poista tiedot, joita et enää tarvitse siihen tarkoitukseen, johon ne on kerätty.

## TOIMENPIDE 4

### VARMISTA KÄSITTELEMIESI HENKILÖTIETOJEN TIETOSUOJA

Jos tallennat tiedot **tietojärjestelmään**, estä sivullisten pääsy tietoja sisältäviin tiedostoihin esimerkiksi salasanalla. Päivitä säännöllisesti järjestelmäsi tietoturva-asetukset.

(Huomaa: yleisessä tietosuojaa-asetuksessa ei säädetä minkään tietyn tietojärjestelmän käytöstä).

Jos säilytät henkilötietoja sisältäviä fyysisiä asiakirjoja, varmista, etteivät valtuuttamattomat henkilöt pääse niihin käsiksi. Säilytä niitä esimerkiksi kassakaapissa tai muussa lukittavassa kaapissa.

## TOIMENPIDE 5

### PIDÄ KIRJAA TIETOJENKÄSITTELYTOIMISTASI

Laadi lyhyt asiakirja, jossa kuvaillet, millaisia henkilötietoja sinulla on ja mihin tarkoituksiin niitä säilytetään. Kansallinen tietosuojaviranomainen saattaa pyytää sinulta asiakirjoja,

joissa on alla luetellut tiedot.

TIEDOT	ESIMERKKEJÄ
Tietojenkäsittelyn tarkoitus	Erikoistarjousten lähettäminen asiakkaille/kotiinkuljetukset, maksut toimittajille, työntekijöiden palkkojen ja sosiaaliturvamaksujen maksaminen
Henkilötietotyytit	Asiakkaiden yhteystiedot, toimittajien yhteystiedot, työntekijätiedot
Käsiteltävät henkilötietoryhmät	Työntekijät, asiakkaat, toimittajat
Vastaanottajaryhmät	Työvoimaviranomaiset, veroviranomaiset
Säilytysajat	Työntekijöiden henkilötiedot työsopimuksen keston (ja lakisääteisten velvoitteiden edellyttämän) ajan; asiakastiedot asiakas-/sopimussuhteen keston ajan
Tekniset ja organisatoriset turvatoimet henkilötietojen suojaamiseksi	Säännöllisesti päivitettävät tietojärjestelmät, lukitut kaapit/kassakaapit
Tieto siitä, siirretäänkö henkilötietoja vastaanottajille EU:n ulkopuolelle	EU:n ulkopuolella sijaitseva henkilötietojen käsittelijä (esim. tietojen tallennus pilveen)

## TOIMENPIDE 6

### VARMISTA, ETTÄ ALIHANKKIJAT NOUDATTAVAT SÄÄNTÖJÄ

Jos olet ulkoistanut henkilötietojen käsittelyn toiselle yritykselle, käytä vain sellaisia palveluntarjoajia, jotka voivat taata tietojenkäsittelyn tapahtuvan yleisen tietosuojaa-asetuksen mukaisesti (esimerkiksi

turvatoimien osalta). Tarkista ennen sopimuksen tekemistä, onko yritys jo mukauttanut käsittelymenetelmänsä vastaamaan yleisen tietosuojaa-asetuksen säännöksiä. Kirjaa velvoite myös sopimukseen.

## TOIMENPIDE 7

### TARKISTA, KOSKEVATKO SEURAAVAT SÄÄNNÖKSET SINUA

> Henkilötietosuojan parantamiseksi organisaatioiden on nimitettävä tietosuojavastaava. **Tietosuojavastaavaa ei kuitenkaan tarvitse nimittää**, jos henkilötietojen käsittely ei kuulu yrityksen ydinliiketoimintaan, ei aiheuta riskiä eikä ole laajamittaista.

Jos yrityksesi esimerkiksi kerää asiakastietoja vain kotiinkuljetuksia varten, tietosuojavastaavaa ei tarvitse nimittää.

Jos tietosuojavastaavaa tarvitaan, hän voi olla yrityksen työntekijä, joka hoitaa tehtävää oman työnsä ohella. Yritykset voivat myös nimittää ulkopuolisen konsultin, samalla tavalla kuin organisaatiot saattavat käyttää ulkopuolisia tilintarkastajia.

> **Yleensä tietosuojaa koskeva vaikutustenarviointi ei ole tarpeen**

Vaikutustenarviointi on tarpeen vain, jos käsittelyyn liittyy korkeampi riski, esimerkiksi kun kyse on julkisen alueen laaja-alaisesta valvonnasta (esim. videovalvonta).

Jos pienyritys käsittelee työntekijöiden palkanmaksua koskevia tietoja ja asiakasluetteloita, tietosuojaa koskevaa vaikutustenarviointia ei tarvitse tehdä.

## Sakot

Tietosuojaviranomaiset voivat määrätä tietosuojasääntörikkomuksista seuraamuksia. Ne voivat määrätä korjaavia toimenpiteitä (kuten antaa keskeyttämismääräyksen tai keskeyttää käsittelyn tilapäisesti) tai sakkoja.

Sakkopäätöksen on oltava oikeasuhteinen, ja sen on perustuttava kaikkien tapauskohtaisten olosuhteiden arviointiin.

Viranomaisten määräämän sakon suuruus riippuu tapauskohtaisista olosuhteista, kuten rikkomuksen vakavuudesta tai sen tahallisuudesta tai tuottamuksellisuudesta. Myös yrityksen asenne ja aikomukset otetaan huomioon.

## Lisätietoa:

### 1. Euroopan komission verkko-ohjeistus tietosuojauudistuksesta – saatavana kaikilla EU-kielillä:

[europa.eu/dataprotection/fi](http://europa.eu/dataprotection/fi)

### 2. Kansallinen tietosuojaviranomainen:

[edpb.europa.eu/about-edpb/board/members\\_fi](http://edpb.europa.eu/about-edpb/board/members_fi)

## TÄRKEÄ TIEDOTE

Tässä oppaassa annettujen tietojen tarkoituksena on edistää EU:n tietosuojasääntöjen tuntemusta.

Asiakirja on tarkoitettu ainoastaan ohjeeksi, ja ainoastaan yleisen tietosuoja-asetuksen teksti on lainvoimainen. Näin ollen vain asetuksella voidaan luoda oikeuksia ja määrätä velvollisuuksia luonnollisille henkilöille. Ohjeilla ei luoda täytäntöönpanokelpoisia oikeuksia tai odotuksia.

Euroopan unionin tuomioistuimella on yksinomainen toimivalta tulkita EU:n lainsäädäntöä sitovasti. Ohjeissa esitetyt näkemykset eivät ennako komission mahdollista kantaa unionin tuomioistuimessa.

Euroopan komissio tai sen puolesta toimivat henkilöt eivät ole vastuussa siitä, miten tämän oppaan sisältämiä tietoja käytetään.

Asiakirja heijastelee sen laadintahetkellä vallitsevaa tilannetta, ja sen sisältöön voidaan tehdä parannuksia tai muutoksia ilman ennakoilmoitusta.



Luxemburg: Euroopan unionin julkaisutoimisto, 2018

© Euroopan unioni, 2018

Uudelleenkäyttö on sallittua, kunhan lähde mainitaan.

Print

ISBN 978-92-79-85383-8

doi:10.2838/683440

DS-02-18-544-FI-C

PDF

ISBN 978-92-79-85404-0

doi:10.2838/230776

DS-02-18-544-FI-N